EXHIBIT 3

Business Associate Agreement

This Business Associate Agreement ("Agreement") is effective as described below by and between Press America, Inc., an Illinois corporation, headquartered at 661 Fargo Avenue Elk Grove Village, IL 60007 (hereinafter called "Vendor") and CVS Pharmacy, Inc. on behalf of itself and its affiliates, including its pharmacy benefits management and retail divisions ("CVS") for which Vendor provides services pursuant to one or more service agreements entered into between the parties ("collectively "Service Agreement") and which are governed by (i) the privacy and security regulations of 45 CFR Parts 160-164 ("the HIPAA Rules"), either because CVS is a covered entity or business associate under those Rules, and (ii) any other applicable federal or state privacy laws and standards, including the Personal Card Information Data Security Standards and the Identity Theft Red Flag Rule (16 CFR Part 681) ("Red Flag Rule") ((i) and (ii) collectively, "Privacy Laws").

CVS and Vendor mutually agree to the terms of this Agreement in order to comply with the HIPAA Rules and other applicable Privacy Laws.

This Agreement is effective as of October 1, 2011 or the effective date of the Service Agreement if earlier ("the Effective Date").

1.0 Definitions

a. **Breach.**
"Breach" shall mean any acquisition, access, use, or disclosure of Private Information in a manner not permitted by the HIPAA Rules.

b. **Individual.**
"Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g) or other applicable federal or state law.

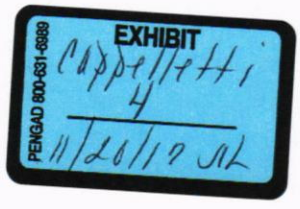
c. **Private Information.**
"Private Information" consists of (1) Protected Health Information ("PHI"), as defined by the HIPAA Rules, created or received on behalf of, or received from Company, (2) Nonpublic Personal Financial Information and, as applicable, Nonpublic Personal Health Information, as defined by the Gramm Leach Bliley Act , and (3) any data or information that (i) relates to an individual and (ii) identifies or there is a reasonable basis to believe it can be used to identify the individual (such as, but not limited to, an individual's name, postal address, email address, telephone number, date of birth, Social Security number, driver's license number, financial account number, or any other unique identifier).

d. **Security Incident.**
"Security Incident" has the same meaning as the term "security incident" in 45 CFR 164.304, and generally means any attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system that stores, transmits, or processes Private Information.

All terms used in this Agreement and not defined elsewhere herein or in the Services Agreement shall have the same meaning as those terms as used or defined in the HIPAA Rules.

2.0 Permitted Uses and Disclosures of Protected Health Information.

a. **Permitted Uses and Disclosures.**
Vendor agrees not to use or disclose Private Information other than as permitted or required by this Agreement or as required by law. Except as otherwise limited by this Agreement, Vendor may use and disclose Private Information in order to provide its services as described in the Service Agreement.



b. **Use and Disclosure for Vendor's Management and Legal Responsibilities.**
Except as otherwise limited in this Agreement, Vendor may use Private Information if necessary for its proper management and administration or to carry out its legal responsibilities. In addition, Vendor may disclose Private Information for its proper management and administration or to carry out its legal responsibilities provided that:

(i) any such disclosure is required by law; or
(ii) (1) Vendor obtains reasonable assurances, in the form of a written agreement, from the person to whom the Private Information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and (2) the person agrees to notify Vendor immediately of any instances of which it is aware in which the confidentiality of the Private Information has been breached.

c. **De-identified Information.**
Vendor may not de-identify Private Information except as necessary to provide its services as described in the Service Agreement. Vendor is prohibited from using or disclosing such de-identified information for its own purpose without the explicit written permission of CVS.

3.0 Obligations of Vendor with respect to Private Information

a. **Safeguards.**
Vendor shall maintain a comprehensive written information security program that is consistent with industry best practices and in compliance with applicable Privacy Laws, including implementing appropriate administrative, technical, and physical safeguards to maintain the security and confidentiality of Private Information, and the security, confidentiality, integrity, and availability of electronic Private Information as required by the HIPAA Rules. Such safeguards shall at least meet the standards described in Schedule A. Without limiting the generality of the foregoing, Vendor shall maintain security policies and procedures, including a Security Incident response plan, data retention, and disposal policies, and a policy and procedure for training of Vendor's employees, agents, and subcontractors on the proper handling of Private Information. The disposal of any documents containing Private Information shall be by means of shredding, erasing or some other means that renders the Private Information unreadable or undecipherable. To the extent that Vendor has access to any part of CVS' data system, Vendor shall comply with CVS' information security policies.

b. **Mitigation.**
Vendor agrees to mitigate, to the extent practicable, any harmful effects of any Security Incident involving Private Information of which it becomes aware.

c. **Reporting Breaches and Security Incidents.**
A. Unauthorized Uses and Disclosures and Security Incidents.
Immediately, but no later than two (2) business days after learning thereof, Vendor shall report any use or disclosure of Private Information not permitted by this Agreement or any successful Security Incident by email to privacyoffice@cvs.com and privacy.officer@caremark.com. This report shall at least:

i. Identify the nature of the use, disclosure or Security Incident;
ii. Identify the Private Information involved;
iii. Identify who made the use or disclosure or caused the Security Incident;
iv. Identify what corrective action Vendor took or will take to prevent further such use, disclosure or Security Incidents;
v. Identify what steps Vendor took or will take to mitigate, to the extent practicable, the harmful effects of the use, disclosure or Security Incident; and
vi. Provide such other information as CVS may reasonably request.

For unsuccessful Security Incidents, the parties agree that Vendor shall provide notice and information on these upon request. A successful Security Incident is defined as any Security Incident that results in the unauthorized use, access, disclosure, modification, or destruction of electronic Private Information. The parties consider the following to be illustrative of unsuccessful Security Incidents when they do not result in actual unauthorized access, use, access, disclosure, modification, or destruction of electronic Private Information: (i) pings on Vendor's firewall, (ii) port scans, (iii) attempts to log on to a system or enter a database with an invalid password or username, (iv) denial-of-service attacks that do not result in a server being taken off-line, and (v) Malware (worms, viruses, etc.).

B. Breaches.
Vendor agrees to report any Breach to CVS immediately, but in no event later than within two (2) business days, after it is discovered (within the meaning of 45 CFR 164.410(a)(2)), and shall provide such information concerning the Breach as requested by CVS to determine whether notifications are required by 45 CFR 164.404, 406 and 408. At a minimum, Vendor shall provide the information concerning the Breach as required under Section 3(c).A above and any other information that may be relevant for CVS to perform a risk assessment to determine whether any notifications should be made. Vendor shall cooperate with and assist CVS in preparing and, if so directed by CVS, sending any notifications that CVS deems necessary or appropriate. Vendor shall be responsible for all costs incurred to make any and all such notifications and for such related costs as specified in Section 5.

d. **Agreements with Agents and Subcontractors.**
Vendor agrees to ensure, through written agreements, that its agents, including any subcontractors, that receive or create any Private Information, agree to the same terms and conditions that apply to Vendor under this Agreement.

e. **Limitations on Further Use and Disclosure.**
Except as provided in Sections 2 (b), Vendor shall not use or disclose Private Information in any manner that would violate the HIPAA Rules, including the Minimum Necessary standard set forth in 45 CFR §164.514(d), if done by a Covered Entity. Vendor further agrees to comply with applicable state and federal privacy and security requirements.

f. **Requests for Access to Information.**
Within five (5) business days of receipt of a request from CVS, Vendor shall provide to CVS or, at its direction, to an Individual, Protected Health Information relating to that individual held by the Vendor or its agents or subcontractors in a Designated Record Set in accordance with 45 CFR §164.524. In the event any Individual requests access to his or her Protected Health Information directly from Vendor, Vendor shall, within five (5) business days of receipt of such request, forward it to CVS. Unless CVS directs otherwise, any response to such request shall be the responsibility of CVS.

g. **Requests for Amendment to Information.**
Within five (5) business days of receipt of a request from CVS, Vendor agrees to make any requested amendment(s) to Protected Health Information held by it or any agent or subcontractor in a Designated Record Set in accordance with 45 CFR § 164.526. In the event any individual requests an amendment to his or her Protected Health Information directly from Vendor, Vendor shall within five (5) business days of receipt thereof, forward such request to CVS. Unless CVS directs otherwise, any response to such requests shall be the responsibility of CVS.

h. **Requests for Accounting of Information.**

Within ten (10) days after Vendor, its agents or subcontractors makes any disclosure of Protected Health Information for which an accounting may be required under 45 CFR §164.528, Vendor agrees to provide in writing via email to privacyoffice@cvs.com and privacy.officer@caremark.com, the information related to such disclosure as would be required for a Covered Entity to respond to a request by an Individual for an accounting in accordance with 45 CFR §164.528. At a minimum, Vendor shall provide CVS with the information specified in 45 CFR § 164.528(b). In the event any individual requests an accounting of disclosures of Protected Health Information directly from Vendor, Vendor shall within five (5) business days of receipt thereof, forward such request to CVS. Unless CVS directs otherwise, any response to such requests shall be the responsibility of CVS.

i. **Requests for Confidential Communications and Restrictions.**
Within five (5) business days of receipt of a request from CVS, Vendor agrees to comply with any request for confidential communication of, or restriction on the use or disclosure of, Protected Health Information held by it or any agent or subcontractor as requested by CVS and in accordance with 45 CFR 164.522. In the event any individual requests a confidential communication or restriction on the use or disclosure of Protected Health Information directly from Vendor, Vendor shall within five (5) business days of receipt thereof, forward such request to CVS. Unless CVS directs otherwise, any response to such requests shall be the responsibility of CVS.

j. **Disclosure of Privacy and Security Practices to Authorities.**
Vendor agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information available to the Secretary of Health and Human Services or his designees or other government authorities in a time and manner designated by CVS or such governmental authorities, for purposes of determining CVS', its customers' or Vendor's compliance with any Privacy Laws.

k. **Background Screening.**
Vendor warrants and represents that Vendor has obtained, at Vendor's own expense and in a manner compliant with all applicable State, Federal and other applicable laws, a "Satisfactory Background Screening," as defined herein below, for all of its employees, agents and subcontractors with access to any Private Information ("Vendor Personnel"). As used herein, a "Satisfactory Background Screening" shall mean, collectively, the following: (1) national federal criminal database check; (2) seven (7) year county of residence criminal conviction search (i.e., search of all counties in which individual has resided within the preceding seven-year period); and (3) in each of (1) and (2) above, containing no felony or misdemeanor conviction that related to fraud or theft (including but not limited to, shoplifting, larceny, embezzlement, forgery, credit card fraud, or check fraud), the disposition of which is within seven (7) years, as allowed by law. Vendor agrees to update such background screening upon reasonable request by CVS, it being agreed that any request based upon the occurrence of any Security Incident or other illegal activity involving Vendor or Vendor Personnel, or the reasonable suspicion of illegal activity involving CVS data, or any regulatory requirements requiring such updates, would be deemed reasonable hereunder.

l. **Documentation.**
Vendor shall maintain documentation of its obligations hereunder to the extent and for the period required by the HIPAA Rules or, if longer, other applicable Privacy Laws. This includes documentation required under 45 CFR 164 Part D, such as documentation to demonstrate that an impermissible use or disclosure of Private Information did not constitute a Breach.

m. **Rights to Private Information.**
Any Private Information provided by CVS, its employees, agents, consultants or contractors to Vendor, or created, obtained, procured, used or accessed by Vendor in CVS' name or on CVS' behalf, shall, as between the parties to this Agreement, at all times be and remain the

sole property of CVS, and Vendor shall not have or obtain any rights therein except as stated herein.

n. **Red Flags.**
To the extent that Vendor provides services in connection with a "covered account" (as such term is defined in 16 CFR 681.2), it shall develop policies and procedures to detect relevant "red flags" (as such term is defined in 16 CFR 681.2) that may arise in the performance of Vendor's activities. Vendor agrees to report any red flags to CVS and to take appropriate steps to prevent or mitigate identity theft.

o. **ARRA.**
Vendor shall comply with each and every obligation imposed on business associates under 42 USC 17921-17954 (Subtitle D of Title XIII of the American Recovery and Reinvestment Act of 2009) ("ARRA"), and each of those obligations is hereby incorporated by reference into this Agreement, with the understanding that compliance with each of those obligations is required under this Agreement only as of the effective date of each of those obligations under ARRA. Without in any way limiting the foregoing, Vendor agrees to comply with (i) 45 CFR Sections 164.308, 164.310, 164.312 and 164.316, and with the additional requirements of ARRA that relate to security and that are made applicable with respect to covered entities, and which are incorporated by reference herein, and (ii) each applicable requirement of 45 CFR 164.504(e) and the additional requirements of ARRA that relate to privacy and that are made applicable with respect to covered entities, and which are incorporated by reference herein.

Medicare Beneficiary Data
Notwithstanding any other provisions of this Agreement, Vendor agrees to comply with:
(i) the requirements specified in the CMS memorandum of December 16, 2008 entitled "Security and Privacy Reminders and Clarification of Reporting Procedures" regarding timely reporting of all security incidents (as defined in the memorandum) involving non-permitted disclosures of personally identifiable information (PII) involving Medicare beneficiaries. Vendor agrees to report such incidents to CVS' Privacy Officer in writing via email at privacyoffice@cvs.com and privacy.officer@caremark.com, within the time frames specified in the CMS memorandum and Attachment, and using the form provided by CMS in the memorandum. Vendor shall be responsible for communicating this reporting requirement to its subcontractors and for reporting any security incidents with respect to PII in the control or possession of such subcontractors.
(ii) to the extent CVS provides written permission for the handling of Private Information by Vendor or its subcontractors outside the United States pursuant to Section 7(e) below, Vendor agrees to comply with the requirements of CMS memorandum of July 23, 2007 entitled " Sponsor Activities Performed Outside of the United States (Offshore Subcontracting)" with respect to Private Information of Medicare beneficiaries, and agrees to incorporate by reference herein the terms specified in the attestation contained in that CMS memorandum.

4.0 Term and Termination.

a. The term of this Agreement shall continue for so long as the Service Agreement remains in effect, except that Section 4(c) shall survive after the termination of the Service Agreement for as long as Vendor retains any Private Information.

b. Upon CVS' determination that Vendor has violated or breached a material term of this Agreement, CVS may either: (1) provide an opportunity for Vendor to cure the breach or end the violation, and terminate this Agreement and the Service Agreement if Vendor does not cure the breach or end the violation within the time specified by CVS; or (2) immediately terminate this Agreement and the Service Agreement if it determines that Vendor has

breached a material term of this Agreement and cure is not possible; or (3) if it determines that neither termination nor cure is feasible, report the violation to the Secretary.

c. **Effect of Termination**

(1) Except as provided in paragraph (2) of this Section 4(c), upon termination of the Service Agreement for any reason, Vendor shall, at the election of CVS, return to CVS or destroy all Private Information in its possession or that of its subcontractors or agents. Vendor and its agents and subcontractors shall retain no copies of the Private Information.

(2) In the event that returning or destroying the Private Information is infeasible, Vendor shall provide to CVS written notification within ten (10) days after termination of the Service Agreement of the conditions that make return or destruction infeasible. Upon agreement by CVS that return or destruction of the Private Information is infeasible; Vendor shall extend the protections of this Agreement to such Private Information, and limit further uses and disclosures of it to those purposes that make the return or destruction infeasible, for so long as Vendor or its agents or subcontractors hold such Private Information.

5.0 Damages.

The parties agree that the remedies at law for a breach by it of the terms of this Agreement may be inadequate and that monetary damages resulting from such breach may not be readily measured. Accordingly, in the event of a breach by either party of the terms of this Agreement, the other party shall be entitled to immediate injunctive relief. Nothing herein shall prohibit either party from pursuing any other remedies that may be available to either of them for such breach. In addition, in the event a Breach occurs of Private Information in Vendor's or its agents or subcontractors' control that CVS determines requires notification under 45 CFR 164.404, 406 and 408 or applicable state laws, Vendor will to the extent required by CVS: (a) provide for such credit monitoring services as deemed appropriate by CVS for at least twelve (12) months for individuals whose information may have been subject to the Breach; (b) provide for call center staffing and operations to the extent necessary to respond to inquiries by affected individuals during this period; (c) pay for any printing, mailing, postage, and other costs incurred by CVS or others to send notifications of the Breach to affected individuals, media, or government authorities; and (d) to the extent reasonably practicable, determine the location of missing information and/or the party or parties that obtained or may have obtained unauthorized access to such information.

6.0 Indemnification.

Vendor will indemnify and hold harmless CVS and any of its officers, directors, employees, or agents from and against any claim, cause of action, liability, damage, cost, or expense, including reasonable attorneys' fees and court or proceeding costs, arising out of or in connection with any breach of the terms of this Agreement, any Breach of Private Information under the control of Vendor or its agents or subcontractors that requires notification under the HIPAA Rules or state law, or any failure to perform its obligations with respect to Private Information by Vendor, it officers, employees, agents, or any person or entity under Vendor's direction or control.

7.0 Miscellaneous

a. **Amendment.**

Vendor agrees to take such action as CVS deems necessary to amend this Agreement from time to time to comply with the requirements of any Privacy Laws. If CVS disagrees with any such amendment proposed by CVS, it shall so notify CVS in writing no later than fifteen (15) days after receipt of CVS' notice of the amendment. If the parties are unable to agree on an amendment, CVS may, at its option, terminate the Service Agreement.

b. **Regulatory References.**

A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or as amended, and as of its effective date.

c. **Interpretation.**
Any ambiguity in this Agreement shall be resolved to permit compliance with the Privacy Laws.

d. **Conflicts.**
The terms and conditions of this Agreement shall override and control any conflicting term or condition of the Service Agreement. All non-conflicting terms and conditions of the Service Agreement remain in full force and effect.

e. **Jurisdiction and Locus of Information.**
Vendor agrees that it currently does not, and in the future shall not, perform any of its services that involve the use or disclosure of Private Information outside the United States, and neither has transferred, nor will it in the future, transfer Private Information outside the United States under any circumstances without the explicit prior written permission of CVS. Vendor agrees that the above provision shall also apply to Private Information in the possession or control of agents or subcontractors of Vendor, and Vendor shall ensure that its agents and subcontractors agree in writing that they will not transfer Private Information outside the United States without the explicit prior written permission of CVS. Irrespective of where it performs its services or is domiciled, or any other factors affecting jurisdiction, Vendor agrees to be subject to the laws of the United States, including the jurisdiction of the Secretary and the courts of the United States. Vendor further agrees that all actions or proceedings arising in connection with this Agreement shall be tried and litigated exclusively in the United States in a venue in the State whose law governs the Service Agreement, and Vendor waives any available jurisdictional defenses as they pertain to the parties' obligations under this Agreement or applicable law.

f. **Audits.**
During normal business hours, and with reasonable prior notice, CVS or its authorized representatives may audit, monitor and inspect Vendor's and its subcontractors' facilities and equipment and any documents, information, or materials in Vendor's or its subcontractors' possession, custody or control; interview Vendor's employees, agents, consultants, and subcontractors; and inspect any logs or documentation maintained by Vendor to the extent relating in any way to Vendor's obligations under this Agreement. An inspection performed pursuant to this Agreement shall not unreasonably interfere with the normal conduct of Vendor's business. No such inspection by CVS as set forth herein shall relieve Vendor of any of its obligations under this Agreement, all of which shall remain absolute.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed by their respective duly authorized officers or agents as of the Effective Date.

CVS Pharmacy, Inc.	Press America, Inc.
By: Anna M. Umberto	By: Martin D'Amico
Name: Anna M. Umberto	Name: Martin D'Amico
Title: Vice President, Strategic Procurement	Title: President
Date: 11/2/11	Date: 10-31-11

Schedule A
Security Standards

Without limitation of the other terms and requirements of this Agreement, the following is deemed incorporated into the Agreement, and shall be additional security requirements for storing, transmitting and handling of Private Information:

1. Vendor's security safeguards for Private Information must be evaluated and certified by a person holding a Certified Information Security Professional (CISSP) certification as meeting health care industry security best practices. Vendor will perform periodic reviews of its security safeguards to ensure they are appropriate and operating as intended. At a minimum, all safeguards will be assessed for compliance and re-certified by a CISSP at least once a year.

2. Documentation of Vendor's security assessments, including testing and any remediation efforts and CISSP safeguard certification, must be retained for a period of six (6) years or such longer period as required by applicable law.

3. Vendor is strictly prohibited from placing any CVS Information on portable computing/storage devices which are not owned and secured by Vendor. Vendor will take all reasonable, necessary and appropriate measures, including encryption, to ensure that CVS Information stored on Vendor owned and secured devices cannot be accessed by unauthorized/inappropriate individuals.

4. Vendor agrees to comply with all guidance issued by the Department of Health and Human Services ("HHS") regarding security safeguards, including any guidance issued by the Secretary of HHS for rendering Private Information unusable, unreadable, or indecipherable to unauthorized individuals within the meaning of 45 CFR 164.402, and as later revised and/or updated.

5. As healthcare industry security best practices evolve to satisfy the HIPAA Rules and other applicable security standards, Vendor agrees to adjust its safeguards accordingly so that they continue to reflect the then current industry best practices.